CLAIMS

What is claimed is:

1. A cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

multiplexer circuitry having an input stage and an output stage, wherein the keys are provided at the input stage of the multiplexer circuitry;

expansion logic coupled to the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block;

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block.

2. The cryptography engine of claim 1, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block by compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic.

3. The cryptography engine of claim 1, wherein the cryptography engine is a DES engine.

4. The cryptography engine of claim 1, wherein the multiplexer circuitry comprises two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level.

5. The cryptography engine of claim 1, wherein the first bit sequence is less than 32 bits.

6. The cryptography engine of claim 1, wherein the first bit sequence is four bits.

7. The cryptography engine of claim 5, wherein the expanded first bit sequence is less than 48 bits.

8. The cryptography engine of claim 6, wherein the expanded first bit sequence is less than six bits.

9. The cryptography engine of claim 7, wherein the third bit sequence is less than 48 bits.

10. The cryptography engine of claim 8, wherein the third bit sequence is six bits.

11. The cryptography engine of claim 9, wherein the second bit sequence is less than 32 bits.

12. The cryptography engine of claim 10, wherein the second bit sequence is four bits.

13. The cryptography engine of claim 1, wherein the key scheduler performs pipelined key scheduling logic.

14. The cryptography engine of claim 1, wherein the key scheduler comprises a plurality of stages.

15. The cryptography engine of claim 1, wherein the key scheduler comprises a determination stage.

16. The cryptography engine of claim 1, wherein the key scheduler comprises a shift stage.

17. The cryptography engine of claim 1, wherein the key scheduler comprises a propagation stage.

18. The cryptography engine of claim 1, wherein the key scheduler comprises a consumption stage.

19. The cryptography engine of claim 1, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

20. The cryptography engine of claim 1, wherein the multiplexer circuitry is a two-level multiplexer.

21. The cryptography engine of claim 1, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer.

22. The cryptography engine of claim 1, wherein the expansion logic and the permutation logic are associated with DES operations.

23. An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine, the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations;

multiplexer circuitry having an input stage and an output stage, wherein the keys are provided at the input stage of the multiplexer circuitry;

expansion logic coupled to the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block;

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block.

24. The cryptography engine of claim 23, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block by compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic.

25. The cryptography engine of claim 23, wherein the cryptography engine is a DES engine.

26. The cryptography engine of claim 23, wherein the multiplexer circuitry comprises two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level.

27. The cryptography engine of claim 23, wherein the first bit sequence is four bits.

28. The cryptography engine of claim 27, wherein the expanded first bit sequence is less than six bits.

29. The cryptography engine of claim 23, wherein the key scheduler performs pipelined key scheduling logic.

30. The cryptography engine of claim 23, wherein the key scheduler comprises a determination stage.

31. The cryptography engine of claim 23, wherein the key scheduler comprises a shift stage.

32. The cryptography engine of claim 23, wherein the key scheduler comprises a propagation stage.

33. The cryptography engine of claim 23, wherein the key scheduler comprises a consumption stage.

34. The cryptography engine of claim 23, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

35. The cryptography engine of claim 23, wherein the multiplexer circuitry is a two-level multiplexer.

36. The cryptography engine of claim 23, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer.

37. The cryptography engine of claim 23, wherein the expansion logic and the permutation logic are associated with DES operations.